

REMARKS

The above amendment and these remarks are responsive to the Office action of 29 Apr 2005 of Examiner Linh L.D. Son.

Claims 1-22 are in the case, none as yet allowed.

35 U.S.C. 101

Claims 8, 9, 10, 11, 12, 16, 17, and 21 have been rejected under 35 U.S.C. 101.

The Examiner asserts that the claimed invention is directed to non-statutory subject matter, stating "The language still recites the program steps without being implemented by a program or software instruction in a computer medium hardware." Applicants traverse.

Applicants are not claiming just a computer medium hardware in which program instructions are implemented. Rather, they are claiming computer implemented methods and systems which comprise steps or elements which may be instantiated in either program instructions in a computer readable medium or which are hard coded in computer

components. In all of these claims, it is clear that a computer is performing the steps or providing the elements of the invention, and there is no requirement that the steps be implemented by a program or software instructions - though that may be the preferred embodiment. Applicants are not required to give up embodiments where the method steps are executed by hardware components of the computer itself, as distinguished from executing program instructions recorded on a computer readable medium.

However, in each of these claims, applicants have again and additionally amended the preamble to make even clearer that computer implemented method steps are being executed by a digital processor at one end of a VPN connection. The hardware elements recited include virtual private network (VPN) connections and a digital processor. The VPN connection, in particular, is clearly described in Applicants' invention as a hardware element. See Figure 2, and the description of VPN technology at page 2, lines 8-17 which clearly establishes the hardware nature, within the context of the Internet and computing industry, of the term VPN. Further, Claim 17 recites a database, VPN connections and address pools. A pool is a hardware element for storing addresses in an electronic database in an Internet

environment, and this claim relates to configuring such a pool. See Applicants' Figure 2, element 48.

Applicants request, therefore, that the 101 rejection be reconsidered and withdrawn with respect to claims 8, 9, 10, 11, 12, 16, 17, and 21.

35 U.S.C. 103

Claims 1, 12, 13, 16, 18, 19 (and apparently also 14, 15, 20 and 22) have been rejected under 35 U.S.C. 103(a) over Borella et al (U.S. Patent 6,353,614, hereinafter Borella) in view of Jain et al. (U.S. Patent 6,047,325, hereinafter Jain).

Claims 2-7 have been rejected under 35 U.S.C. 103(a) over Borella et al in view of Jain et al, and further in view of Arrow (U.S. Patent 6,226,751).

Claim 11 is rejected under 35 U.S.C. 103(a) over Arrow.

Claims 8-11, and 17 have been rejected under 35 U.S.C. 103(a) over Allied Telesyn, NAT, GRE, and Security

Associations, May 1998, Page 1-5, hereinafter "AT".

Applicants traverse, and argue that the Examiner has not established a *prima facie* case of obviousness, for the reasons set forth hereafter.

Summary of The Present Invention

Applicants invention relates to IP security in a virtual private network using network address translation (NAT) by performing one or a combination of the four types of VPN NAT, including

1. VPN NAT type 'a source-outbound' IP NAT,
2. VPN NAT 'b destination-outbound',
3. VPN NAT type 'c inbound-source' IP NAT, and
4. VPN NAT type 'd inbound-destination' IP NAT.

This involves dynamically generating NAT rules and associating them with manually or dynamically generated (IKE) Security Associations, before beginning IP security

that uses the Security Associations. Then, as IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed.

These 4 types of VPN NAT are defined in the specification at page 17, lines 5-19 (Table 2).

The current invention concerns the ability to define and process multiple VPN NAT rules for a single VPN connection, via the specification of multiple IP addresses (an IP address set) for types of VPN NAT. The term 'VPN' here is used as a synonym for the IP Security protocols ESP (Encapsulating Security Payload) and AH (Authentication Header). Basic references for these protocols are (all from IETF (Internet Engineering Task Force)); IKE RFC2409 , ESP RFC2406, AH RFC2402, and the most basic, on IP Security architecture, RFC2401.

Of course, the subject invention works over LANs and WANs, including wireless; it works wherever IP traffic works. And is embodied in only 1 end of the VPN connection; the VPN implementation at the other end is completely unaware that its peer is performing VPN NAT operations. Even so, it may be embodied in both ends concurrently and

independently, and this is a feature of the current invention.

The problem addressed by the current invention is that IP Sec & NAT are conflicting; a packet with IP Sec applied cannot, in any way, be altered without invalidating the packet. Yet NAT requires that parts of a packet be altered. How can these technologies be made to function together in an integrated fashion, so that the benefits of each can be concurrently obtained?

The key idea (in general terms) that allows integration of VPN & NAT is that the NAT operation is logically performed prior to beginning the IKE negotiation of Security Associations, and is integrated with the start of IKE negotiations. Hence the IKE negotiation begins and proceeds with the NAT IP address(es), rather than actual IP address(es), and no additional steps or devices are required. Hence any possible IP Sec protocol that is applied to a datagram (encryption or digital signature or both) works at both ends, because both IKE (and the resulting Security Associations) & IPsec are using the NAT address(es).

Summary of the Art Cited

Following is a summary of how the present invention differs from cited prior art in 6,353,614 (Borella et al), 6,047,325 (Jain et al), 6,226,751 B1 (Arrow et al), and newly cited art AT (Allied Telesyn, configuration directions, 9 pages, for their 'software release 7.6, revisions 2, May 1998).

Borella describes a method and protocol for Distributed NAT ("DNAT") used to overcome the limited 32-bit address space of IPv4. The protocol includes a port allocation protocol and translates ports as well as IP addresses. Local ports are replaced with globally unique ports, unique for the scope of DNAT. Hence, Borella et al employs what is often referred to as 'PNAT', meaning 'port & network [IP] address translation'. The problems Borella addresses are those seen as inherent in the current versions of NAT (Col. 1, lines 41-67, Col. 2, lines 1-28).

So, some of the differences between Borella et al the subject invention are:

- 1) The subject invention does not translate ports

(transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

- 2) DNAT is a form of PNAT that centralizes the assignment and allocation of ports. Borella has nothing to do with IP Security or the IP Security protocols ESP & AH, nor with IKE. This is critical since the incompatibilities and difficulties of combining of IP Security & NAT are well known (see, for example, IETF RFC3715). Hence Borella et al does even begin to address any of the problems associated with integrating IP Security and NAT. Nor is it a problem Borella is trying to solve.
- 3) The current invention does not use PAP (Port Allocation Protocol) (Col. 5, lines 61-62) or anything similar to PAP. The current invention does not allocate ports at all, using anything.
- 4) Borella does not use or integrate VPN's (IP Sec-based

or otherwise), whereas for the current invention, this is central. Borella does mention VPNs once (Col. 16, lines 20-23), but this is merely an assertion. No description is given, no details, no elaboration. This single sentence does not anticipate, nor does it solve, the problems associated with using and integrating NAT with IP Sec-based VPNs.

Jain describes a network device which translates addresses and ports and filters packets at the link, network and transport layers. The invention uses a table (one of three mentioned) to bind MAC and IP addresses, via ARP (Address Resolution Protocol). Jain does say that traffic can be encrypted and authenticated when the traffic is sent over a wide-area-network. The problem Jain addresses is enabling a scalable virtual LAN (aka 'VLAN') over physical LANs and WANs.

Some differences between Jain and the subject invention are:

- 1) The current invention does not translate ports (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP

traffic does use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

- 2) The current invention does not translate IP address based on MAC addresses as does Jain, nor does it map IP addresses based on MAC addresses (at all) (Col. 6, lines 29-32).
- 3) The current invention does not use ARP, and does not use MAC addresses at all. Hence the current invention solves the functional combination of IPsec-based VPN and NAT in a manner completely different from Jain (if Jain solves it). This is illustrated by the observation that both ends of Jain (Figure 1, elements 26 & 28) must embody Jain, while for the subject invention, only one end of the peer VPN connection embodies the subject invention.
- 4) The mapping of MAC addresses to IP addresses to change apparent physical location of a IP address is the basic technology of VLANs. "If the packet is to be directed to a wide areas network, encryption and authentication

procedures can be provided..." (Col. 2, lines 14-16). This and other passages in Jain suggest the relationship of Jain's use of VPN and Jain's use of network address translation (see for example important detail in Col. 5, lines 24-39). Note that first the packet is unencapsulated (a term commonly used in the context of VPN's) and then later (apparently optionally), a mapping to new MAC is made. In contrast, in the current invention, NAT is integrated with IP Sec.

- 5) Jain does not use IKE to automatically generate security associations.

Arrow describes how a selection of a plurality of (network) entities are coupled to a public data network. The plurality is given identifiers. VPN's can be set up among the plurality that include encryption & authentication & compression. "Another variation on the embodiment includes defining address translation rules for virtual private network units coupled to the public data network" (abstract). The purpose if Arrow is to enable the realization of virtual private networks.

The following sections of Arrow are interesting. "The present invention is not limited to any one particular implementation technique" (Col. 4, lines 66-67). Arrow goes on to say that one of ordinary skill in the art "will be able to implant the invention with various technologies without undue experimentation..." (Col. 5, lines 1-2). All this despite Arrows assertion that "... components implemented by the present invention are described at an architectural, function level.", without details!

Some differences between Arrow and the present invention are:

- 1) The current invention does not select a plurality of entities coupled to the public data network.
- 2) The current invention does not assemble a plurality of identifiers for the plurality of entities.
- 3) The current invention does not use these identifiers to identify communications between the entities.
- 4) The current invention does not assemble the entities into groups.

- 5) It seems that (Col. 12, lines 7-54) any IP Sec that Arrow might employ (no mention) is done before or after (some kind of) NAT for the communication, that is, serially. Hence in Arrow NAT is not integrated with IP Sec.
- 6) Arrow uses port mapping (aka PNAT) (Col. 12, lines 52-54).
- 7) Arrow does not use IKE to automatically generate the IP Sec security associations. Hence Arrow does not teach the use of VPN NAT integrated with IKE and IP Sec.

The present office action includes new prior art:
Allied Telesyn, NAT, GRE, and Security Associations, May 1998, pages 1-5, hereinafter 'AT'. These pages are configuration instructions for some device, and have the headings of 'Configuration Example 3' and 'NAT and security associations'. Both sections (chapters?) contain numbered lists of configuration instructions for connecting (see the two very similar diagrams) two LANs via two routers both connected to the Internet. The configuration instructions are for each router for each LAN.

Some key differences between the current invention and AT are:

- 1) The current invention uses IKE to automatically generate the security associations (this is shown in the current invention claim 1 "... based on IP Sec...") and AT does not. This is clearly shown in AT configuration instructions steps 11-14 for "Router A", 11-14 for "Router B", in the two boxes in the 'NAT and security associations' section (see the line "Manager > create enc key=1 val=random"), in steps 7-10 on the following page for another "Router A", and finally in steps 7-10 for "Router B" on the last page. Note, for example, back in the "NAT and security associations' section 2nd page, the paragraph under subheading "Instructions" where it says "... these keys must be created manually by typing a sequence of commands on a terminal ...". Quite clearly, these security association keys are manual and not created by IKE.
- 2) Another difference is that the NAT rule is created automatically in the current invention and in AT it is

created manually. Again, this can be clearly seen in steps 15-16 for "Router A" and 15-16 for "Router B".

- 3) The current invention does only requires use of VPN NAT at a single end (see for example current invention claims 1, 8 and 11 all of which specify the claim "... at one end ...") of the VPN connection, while the AT document clearly does not. AT requires configuration at both ends. This is see in the configuration of Router A and Router B.

Response to the Office Action Rejections

Referring to paragraph 6 of the Office Action, claims 1, 12, 13, 16, 18, 19 are rejected "as being unpatentable over Borella ... In view of Jain."

With respect to claims 1, 12, 13-16, 18, 19, 20 and 22, in paragraph 7 of the Office Action the Examiner states the implementation of NAT with VPN has also "been considered in Borella col 16, 20-23". One sentence in Borella is not a solution, it is not a description, it is not a design; it is merely a unsubstantiated assertion which falls far short of

suggesting Applicants' invention.

And, even if taken at face value, Borella is still irrelevant to the current invention because of the differences summarized above and repeated here: Borella translates ports and the current invention does not, Borella uses DNAT and the current invention does not, Borella uses PAP and the current invention does not.

Further distinguishing the current invention claim 1, Borella invention does not work at one end only of a VPN connection (e.g. PAP), Borella does not do configuring a NAT IP address pool, Borella does not configure a VPN connection to utilize said NAT IP address pool, Borella does not obtain a specific IP address from said NAT IP address pool, Borella does not start said VPN connection, Borella does not load into an operating system kernel IP Sec security association and connection filters, and lastly Borella does not apply VPN NAT to said IP datagram.

The Examiner states Jain teaches the VPN connection set up utilizing DHCP. This is not what Jain does and even if it were it is completely irrelevant to the current invention. Jain col 5, 13-39 does not 'teach VPN

connection setup utilizing the DHCP'. What Jain uses DHCP for is, is the same thing everyone that uses DHCP uses it for, which is what is was designed to do. And it simply does not do VPN connection setup.

What Jain states (Col. 5, lines 19-25) is "Additional security may be provided by binding machines to both MAC and IP addresses and having filters that check both the MAC and IP address of a source of a message. Such binding may be performed using domain name servers (DNS) and ... DHCP." This is completely irrelevant to the current invention on many levels and in many ways. And the fact that in a later step of Figure 7 a packet is "unencrypted and decapsulated" (Col. 5, line 29) is irrelevant for the simple reason that this is clearly after the use of DHCP for anything.

Thus, Jain is not setting up a VPN connection, the phrase 'additional security' does not refer to IP Sec, VPN security associations or anything remotely related to it. The binding of MAC and an IP is irrelevant to the current invention and irrelevant to VPN, irrelevant to IP Sec. The fact that this binding is done with DHCP or DNS or both is even further irrelevant to the current invention, irrelevant to VPN, irrelevant to IP Sec. In the current invention VPN

connection setup involve IKE and associated protocols for the automatic generation of the IP Sec security associations. This cited section is also completely irrelevant to IKE, the IKE protocols and security association generation. Hence, Applicants traverse the Examiner's assertion that "Jain teaches the VPN connection set up utilizing DHCP".

The Examiner then states, "Therefore, it would be obvious ... to incorporate Borella's NAT ... with Jain's VPN connection method..." Applicants traverse. The paragraph above refutes the basis for this sentence and the 'therefore'. Another reason for non-obviousness of combining or incorporating Borella with Jain is the fact the although they use NAT, they use very different types. As mentioned earlier, Borella uses DNAT which also translates the 'address' used in the layer above the network layer (the TCP or UDP port), while Jain's NAT involves the mapping of the layer below the network layer (the MAC address). Of course, the reason for Borella using the above layer address and Jain using the below layer address is that they solve very different problems. This makes it more non-obvious to incorporate one with the other. And of course neither tries to solve the problem of integrating NAT with IP Sec-

based VPN's as does the current invention.

The Examiner then states next "Since, Borella anticipated the implementation of NAT with VPN...". Applicants traverse. As explained above, Borella does no such thing.

The Examiner then states next "...further, Jain's invention utilizes DHCP servers". This is quite irrelevant to the current invention, which does not use, nor rely on, nor disallow such.

The Examiner then states, "The incorporation of NAT in Jain's DHCP server would allow the VPN connection to be executed on one end of the connection." Applicants traverse. This is quite technically incorrect; an IP Sec-based VPN most assuredly must be 'executed' at both ends. Please see the previously referenced RFC's that describe IP Sec protocols. This is also a misreading of the current invention which states that (claim 1) '...steps executed at one end of the VPN connection of...' then lists 7 steps which are occurring at one end of that VPN connection. The connection filters and security associations for the VPN connection, and of course the IP Sec protocol processing

itself, are occurring at both ends of the VPN connection.

With respect to claims 14 and 15, the Examiner states, "Borella does teach the implementation of NAT with VPN...". Applicants traverse. Borella does no such thing. As stated above, the referenced single sentence in Col. 16, lines 20-23 does not teach anything. It is mere assertion. There is no description, no figure, no detail, no claims, nothing in Borella that 'teaches' one of ordinary skill in the art the implementation of NAT with VPN.

The Examiner then states 'Therefore, ...'. This sentence does not follow at all from the previous sentence since the previous sentence is refuted.

The Examiner then cites Borella (Col. 5, lines 5-14 to support the idea that 'ICMP ... implementation in NAT can also be implemented in the VPN NAT environment'. Applicants traverse. Borella does not show this at all for a number of reasons.

First, note that current invention claim 14 is about performing VPN NAT "on" ICMP datagrams. In Borella, the cited section talks about how PAP "is implemented in a

separate PAP layer or as an integral part of ICMP". This is not performing NAT of any kind on ICMP. Further, it cannot be performing Borella's type of PNAT because ICMP packets do not have ports! Hence the ports cannot be translated. Hence Borella has nothing to do with NAT of ICMP and no bearing on VPN NAT of ICMP as claimed in claim 14 of the current invention.

The Examienr also asserts, "... FTP implementation in NAT can also be implemented in the VPN NAT environment" citing Borella at Col. 2, lines 22-28. Applicants traverse. The reference merely stated the FTP can be NATed. It says nothing about VPN NAT which is what current invention claim 15 is about. There is nothing in Borella that allows the leap from NAT to VPN NAT.

With respect to claims 2-7, the Examiner asserts [Paragraph 9 of the Office Action] that claims 2-7 are unpatentable over Borella in view of Jain and further in view of Arrow.

Claim 2 is dependent on claim 1 and adds 'said VPN connection is configured for outbound processing, and said applying step comprises outbound source IP NATing'.

Applicants have already explained how Borella and Jain are very different from the current invention claim 1.

Neither perform outbound source IP NATing. Hence they have no bearing on claim 2. The differences between the current invention and Arrow are discussed above. Arrow also does not do outbound source IP NATing.

Claim 3 depends on claim 1 and adds some combination of inbound source IP NATing or outbound destination IP NATing. It has already been shown how Borella and Jain are very different from the current invention claim 1. And none of the cited prior art do these claim 3 actions.

Claim 4 depends on claim 1 and adds manually-keyed IP Sec with VPN NATing. Borella, Jain & Arrow do not read on claim 1, and none of the cited prior art do the steps set forth in claim 4.

Claim 5 depends on claim 1 and adds IKE-generated keying with VPN NATing. Claim 1 has been distinguished and none of the cited prior art does what claim 5 adds.

Claim 6 depends on claim 1 and adds creating a message for IKE which in turn uses the IP address from the NAT IP

address pool in negotiating the security association keys.

Claim 1 has been distinguished and none of the cited prior art does the steps added by claim 6.

Claim 7 depends on claim 6 and adds IP sec key creation and loading of resulting security association into OS kernel. Claim 6 has been distinguished and none of the cited prior art does the steps added by claim 7.

At paragraph 10 of the Office Action, the Examiner rejects claims 2-7. Applicants have responded to these rejections above.

Claim 11 has been rejected over Arrow. Applicants traverse.

Arrow (Col. 10, lines 17-20) does not 'generate journal records responsive to VPN connection' as stated claim 11. The cited section concerns SNMP, a well-established system management protocol which can be trivially seen to not generate journal records at all, of any kind, and hence does not generate journal records responsive to VPN connection. SNMP also does not update journal records. SNMP will update its appropriate MIB OIDs for each datagram processed through

a VPN connection (if the right level of SNMP is implemented on the system, and the appropriate MIBs are implemented). Updating a MIB OID is not the same as updating a journal record with new records. And finally SNMP does not enable a customer to manage the journal records. SNMP has nothing whatsoever to do with journal records.

The Examiner concludes that "... It is obvious at the time of the invention was made... that the same protocol includes the claim feature completely". Applicants traverse.

Since the SNMP protocol (version 1, 2 or even the current 3) does not at all include generating journal records, it does not, responsive to anything, add records nor enable the management of records. Again, the SNMP protocol has nothing to do with journal records. (Basic SNMP references appropriate to the current invention include IETF RFC1442, RFC1450, RFC1902.)

Claims 8-11 and 17 have been rejected over Allied Telesyn, NAT, GRE and Security Associations, May 1998, p1-5.

Applicants traverse. The AT reference does not utilize

IKE, and the integration of NAT with IKE and IP Sec-based VPNs is the whole point of the present invention.

With respect to claim 8, AT does not disclose "A method ... of IP Sec-based VPN ... at one end of a VPN connection" because AT does not implement or support or describe or use IP Sec-based VPN as used by the current invention.

IP Sec-based VPN means using IKE and IP Sec (ESP & AH). AT does not use IKE at all. Further, AT does not do anything "at one end" as does the current invention. AT clearly and explicitly requires configuration at both Router A and Router B. Further, AT does not configure anything "... for each of the three types of VPN NAT", and AT does not configure "a remote IP address pool".

The Examiner states [Page 6 of the Office Action], "...that it would be obvious at the time of the invention ... to realize that the configuration script for either Router A ... and Router B does teach the three type of VPN NAT...".

Applicants traverse. This is most certainly not the case, it is not obvious, since AT does not use IKE to

automatically generate its security associations. Instead AT generates the security associations manually, by a series of commands on a command line. A person using AT would not be using IKE, hence would not know IKE, nor understand the implications of using IKE, and such a person would not find it obvious at all, that NAT can be integrated with IKE and IP Sec protocols, as the current invention claims. Please see RFC2409 to appreciate just how absolutely non-obvious it is to integrate NAT with IKE and IP Sec. Especially when not even using IKE!

The Examiner states [Page 6 of the Office action] "The type a outbound source IP NAT, VPN NAT type c inbound source IP NAT is implied [in AT] on page 3-4 #10-16, and Page 4-5 #10-16...". Applicants traverse.

The referenced items 10-16 pages 3-4 do not refer to NAT. Items 11-14 concern security associations only and have nothing whatsoever to do with NAT (of any kind). Hence 11-14 on pages 3-4 and pages 4-5 have nothing at all to do with VPN NAT type a or type c. Item 15 on pages 3-4 and pages 4-5 mentions NAT like this: "Enable the NAT module" and "enable ip nat". Hence item 15 is completely generic, and contrary to the Examiner's statement, OA does not

"imply" type a outbound source VPN NAT nor VPN NAT type c inbound. Item 16 on pages 3-4 and on page 5 mentions "dynamic ENAT", and says "there are other ways to configure NAT". How is one to get from these words to 'type a outbound source VPN NAT or type c inbound source'?? ENAT is nowhere defined in AT, so could mean lots of things.

Applicants traverse the suggestion of the Examiner that the leap from dynamic ENAT is obvious to one of ordinary skill in the art, without even using IKE.

The Examiner states [page 6 of the Office Action], "VPN NAT type d inbound destination IP NAT is implied on pages 3-4 lines 10-16". (Sic. Applicants are sure the Examiner meant items 10-16 and not lines 10-16, and assume that in what follows.) Applicants traverse.

Items 10-14 have nothing whatsoever to do with NAT, of any kind. Hence they have nothing to do with VPN NAT type d. Item 15 is the same completely generic reference to NAT mentioned above ("Enable the NAT module" and "enable ip nat"), and so is also useless in implying VPN NAT type d. The last item, 16, was just discussed. It does not, at all, "imply" VPN NAT type d. This is for the same reasons stated above; ENAT is undefined, the definition of VPN NAT is

directly related to IKE. AT is not even using IKE.

Therefore, it is not implied.

The Examiner then states, "... AT does disclose a method to enable GRE for ...". Yes AT uses generic routing encapsulation. (It is not specified at what RFC level; most likely it is RFC1702 since RFC2784 wasn't published until 2000, and the AT document is dated May 1998.) Applicants traverse.

GRE is completely irrelevant to the current invention. Completely. So, for example, even if GRE somehow suggests or implies or has a policy database as the Examiner assumes when he states "... the policy database must exist", it is still irrelevant. A policy database useful for GRE is completely different from the policy database referenced in the current invention claim 8. And, more importantly, the GRE specification does not define or suggest a policy database. So the fact the AT uses GRE does not make any aspect of claim 8 obvious.

With respect to claim 9 and 10, the Examiner states that AT 'discloses the method claim 8...'. Applicants traverse.

AT does not disclose the method of claim 8 as shown above.

The Examiner then quotes claim 9 of the current invention and adds "p3 #12-13, and #7" in AT. AT items 12 & 13 concern configuration of the security association, as clearly AT states. They clearly have nothing at all to do with a remote IP address pool as referenced in claim 9 or the server IP address pool of claim 10. Yes, both items reference 'IP address ranges'. But configuring a range of IP addresses for a security association does not imply or suggest an IP address pool for VPN NAT. A security association is not that same as IP address pool for VPN NAT. They both just happen to use multiple IP addresses. As do other networking applications and contexts. Item 7 is about GRE, and only says enable GRE, and hence has nothing whatsoever with remote IP address pools.

With respect to claim 11, the Examiner cites AT p3 item 11. Applicants traverse.

AT item 11 concerns creating a security association. While it is true the VPN connections in the current

invention rely on security associations, as generated by IKE, a security association is not the same as a VPN connection. And creating a security association is not the same as VPN connection configuration, nor of course is it the same as the traffic processed through a VPN connection. And, even beyond these differences is, the 'generating journal records', and 'updating journal records' which are also completely absent in AT. Item 11 and everywhere. Hence item 11 is irrelevant to claim 17.

Applicants request, therefore, that the rejection of claims 1-22 under 35 U.S.C. 103 be reconsidered and withdrawn.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the

Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. Boden, et al.

By

Shelley M Beckstrand
Shelley M Beckstrand
Reg. No. 24,886

Date: 27 Aug 2005

Shelley M Beckstrand, P.C.
Attorney at Law
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545